UNITED STATES DEPARTMENT OF HOMELAND SECURITY
TRANSPORTATION SECURITY ADMINISTRATION
STATEMENT OF JUSTIN P. OBERMAN
ASSISTANT ADMINISTRATOR,
SECURE FLIGHT/REGISTERED TRAVELER

SUBCOMMITTEE ON ECONOMIC SECURITY, INFRASTRUCTURE PROTECTION, AND CYBERSECURITY
COMMITTEE ON HOMELAND SECURITY
UNITED STATES HOUSE OF REPRESENTATIVES

June 29, 2005

Good morning Mr. Chairman, Congresswoman Sanchez, and Members of the Subcommittee. I am pleased to have this opportunity to appear before you today on behalf of the Transportation Security Administration (TSA) to discuss our efforts and challenges relating to improving pre-screening of aviation passengers against terrorist and other watch lists, particularly in the context of our Secure Flight Program. The Department of Homeland Security (DHS) and TSA are committed to the development of Secure Flight as an essential layer in our system of systems approach to aviation security. We envision Secure Flight as a unique opportunity to leverage technology and information management practices to implement a program that enhances the security of the civil aviation system. An additional benefit of Secure Flight is the prospect for improving and facilitating travel for the broad public. We are working to quickly resolve remaining policy, technical, cost, and privacy considerations.

BACKGROUND

Currently, aircraft operators are required to compare the name of each passenger to the names of individuals on two Federal Government watch lists known as the No-Fly and Selectee Lists. When an aircraft operator has a reservation from a passenger with a name that is the same as, or similar to, a name on the No-Fly list, the aircraft operator is required to notify law enforcement personnel and TSA to verify whether that passenger is in fact the individual whose name is on either list. If the passenger is verified as an individual on the No-Fly List, the aircraft operator is prohibited from transporting the passenger and all accompanying passengers. When an aircraft operator has a reservation from a passenger with a name that is on the Selectee List, the aircraft operator is required to identify the individual to TSA for enhanced screening at security screening checkpoints.

In addition, domestic air carriers perform passenger pre-screening through their use of the Computer-Assisted Passenger Prescreening System (CAPPS). CAPPS, which was developed jointly by the airlines and the Federal government in the mid-1990s, analyzes information in passenger name records (PNRs) using certain evaluation criteria to

determine whether a passenger and his property should receive a higher level of security screening prior to boarding an aircraft.

As part of the Aviation and Transportation Security Act (ATSA) (P.L. 107-71), Congress directed that the Secretary of Transportation ensure that "the Computer-Assisted Passenger Prescreening System, or any successor system – is used to evaluate all passengers before they board an aircraft; and includes procedures to ensure that individuals selected by the system and their carry-on and checked baggage are adequately screened." This requirement became part of the mission of TSA, with overall responsibility transferring with TSA to DHS on March 1, 2003, as provided for in the Homeland Security Act of 2002 (P.L. 107-296).

The need to expedite implementation of an effective passenger pre-screening system was reinforced and reemphasized in the final report of the National Commission on Terrorist Attacks Upon the United States (9/11 Commission), which states at page 392:

> "[I]mproved use of "no-fly" and "automatic selectee" lists should not be delayed while the argument about a successor to CAPPS continues. This screening function should be performed by TSA and it should utilize the larger set of watch lists maintained by the Federal Government. Air carriers should be required to supply the information needed to test and implement this new system."

Spurred by the recommendations of the 9/11 Commission, Congress enacted in relevant part Section 4012 of the Intelligence Reform and Terrorism Prevention Act of 2004 (IRTPA)(P.L. 108-458). The provision directs that TSA commence testing of and ultimately assume responsibility for "the passenger prescreening function of comparing passenger information to the automatic Selectee and No Fly lists [utilizing] all appropriate records in the consolidated and integrated terrorist watch lists maintained by the Federal Government in performing that function."

Secure Flight is TSA's program to move the existing watch list vetting process of domestic passengers from the air carriers into the Federal Government in order to make the process more effective, consistent, and efficient for the traveling public from a security and customer service standpoint. Under this program, TSA will assume the function of conducting pre-flight comparisons of domestic passenger information to Federal Government watch lists, to include expanded versions of the No-Fly and Selectee Lists. TSA is also reviewing whether the Secure Flight system may be able to incorporate a streamlined version of the existing CAPPS system to evaluate information in PNRs that passengers otherwise provide to aircraft operators in the normal course of business.

BRIEF OVERVIEW OF SECURE FLIGHT'S GOALS

The importance of an effective Secure Flight program is hard to overstate. Because the airlines have varying systems by which they implement passenger prescreening, the

effectiveness, efficiency, and consistency in response for airline passengers of the current system is limited. In developing Secure Flight, TSA is seeking that greater effectiveness, efficiency and consistency, but doing so requires the consolidation of functions that are now being carried out separately by 65 air carriers, for 1.8 million passengers on 30,000 flights fly each day, at approximately 450 airports where security screening is required. Once implemented, however, Secure Flight would enable TSA to better focus its resources and security screening efforts on those passengers who are identified to be more likely to pose a threat to aviation security. In addition to resulting in a more secure system, the benefits to legitimate travelers, who comprise the vast majority of the traveling public, will be evident. TSA fully appreciates the frustration felt by individuals posing no threat to aviation security who are selected for additional scrutiny at airports because of a false positive report that they match or resemble a name on a watch list. Once operational, Secure Flight will result in fewer individuals undergoing additional scrutiny, thus reducing one element of the "hassle factor." Furthermore, by reducing false positives, additional passengers will be able to avail themselves of expedited check-in procedures on the Internet and at self service ticket kiosks. The overall result would be a more secure system that is also more efficient and user-friendly to travelers.

In assuming the watch list checking role from the air carriers, we recognize that they are indispensable partners, without whom the Secure Flight program will not succeed. The carriers have been extremely cooperative, for example, in providing the necessary historic PNR data relating to domestic flights in June, 2004 to enable TSA to conduct its preliminary testing, and we expect that this cooperation will continue as we make preparations for beginning operational testing of Secure Flight. We are also partnering with U.S. Customs and Border Protection (CBP) on the transmission of passenger data because most domestic carriers already have pre-existing information technology connections to CBP relating to passenger data.

TSA also acknowledges that carriers are concerned with not only the technical issues relating to connectivity but also with the initial start-up costs that they might have to bear. TSA will continue to work with the airline industry to develop cost estimates for implementation and continued operations and is committed to working with the carriers in managing the start-up costs of Secure Flight, including the costs associated with aligning the IT systems. However, ultimately, the anticipated economies of scale that will be achieved by consolidating the watch list vetting function into the government, a function whose attendant costs are currently borne by the carriers, will likely lead to significant savings to the carriers. An additional benefit of Secure Flight is that the increased efficiency that it will afford at checkpoints and ticket counters should assist carriers in maintaining and improving passenger satisfaction and customer service—objectives that we share with the carriers as TSA carries out its primary mission of ensuring civil aviation security.

TERRORIST WATCH LISTS AND FUNCTIONALITY OF SECURE FLIGHT

Before I discuss further our efforts to develop and test Secure Flight and the issues that must be resolved prior to its actual deployment, please allow me to provide some

information regarding the underlying terrorist databases on which passenger information will be compared. Homeland Security Presidential Directive 6 (HSPD-6) and an accompanying Memorandum of Understanding (MOU) dated September 16, 2003, directed the creation of the Terrorist Screening Center (TSC) and reengineered the terrorist watch list process.

Since its creation on December 1, 2003, TSC has developed and maintained the Federal government's Terrorist Screening Database (TSDB). TSDB receives international terrorist-related identity data from the National Counterterrorism Center (NCTC), also created under HSPD-6, and purely domestic terrorist information from the FBI. The NCTC receives nominations from U.S. Government agencies, such as CIA and FBI, for placement on specific Federal watch lists. The NCTC then creates records in its terrorist identities database and forwards the originator nomination to the TSC. The TSC then provides unclassified identity data to TSA for use in its No- Fly and Selectee lists, based on specific No-Fly and Selectee nominations from agencies. TSA personnel at the TSC provide quality assurance and monitor the transmission of this data.

Currently, TSA's role is to provide the No Fly and Selectee lists to foreign and domestic air carriers that service U.S. airports. TSA has provided the air carriers with guidance on how to handle and operate the lists via Security Directives and Emergency Amendments, and TSA's 24x7 watch centers take air carrier reports and coordinate No-Fly and Selectee operational issues. TSA continues to work closely with TSC to ensure as much as possible that the watch lists are accurate and comprehensive. Additionally, TSA maintains a list of cleared individuals whose names are similar to those contained in the watch lists. Cleared lists with identifying information are attached to the No Fly and Selectee lists to assist carriers in distinguishing between watch listed and non-watch listed passengers.

Secure Flight will involve the comparison of passenger information for domestic flights to names in the TSDB maintained by the TSC, including the TSA No-Fly and Selectee Lists, to identify individuals known or suspected to be engaged in terrorist activity. Secure Flight will automate the vast majority of watch list comparisons, will allow TSA to apply more consistent procedures where automated resolution of potential matches is presently not possible (due to the current reliance on separate procedures at each airline), and will allow for more consistent response procedures at airports for those passengers identified as potential matches.

Bringing the watch list matching function into the Federal government will also permit expansion of these lists to include sensitive information that could not be disclosed to the airlines. Under the current system, TSA has great concerns over the security aspects of providing air carriers and many of their employees with information contained on the No-Fly and Selectee Lists. These security concerns would be reduced once the Federal government assumes the responsibility for administering watch list comparisons, thus permitting integration and consolidation by TSC of additional information relating to individuals known or suspected to be engaged in terrorist activity.

PROGRESS AND CHALLENGES

On September 24, 2004, TSA published in the *Federal Register* a number of documents necessary to allow the agency to begin testing the Secure Flight program. These included: (1) a proposed order to U.S. aircraft operators directing them to provide a limited set of historical passenger name records (PNRs) to TSA for use in testing the program (69 FR 57342); (2) a Privacy Act System of Records Notice (SORN) for records involved in testing the program (69 FR 57345); and (3) a Privacy Impact Assessment (PIA) of program testing (69 FR 57352). These documents explained that in addition to testing TSA's ability to conduct automated watch list comparisons for purposes of the Secure Flight program, TSA intended to conduct a separate test to determine whether the use of commercial data would be effective in identifying passenger information that is incorrect or inaccurate. TSA updated the SORN and PIA on June 22, 2005 (70 FR 36320).

On November 15, 2004, TSA published in the *Federal Register* a document setting forth, among other things: TSA's response to public comments on the September 24, 2004, proposed order; revisions made to the proposed order in response to comments; and the text of the final order. (69 FR 65619). The final order directed U.S. aircraft operators to provide to TSA, by November 23, 2004, a limited set of historical PNRs for testing of the Secure Flight program.

Utilizing the data provided by air carriers, TSA commenced testing of the watch list matching function for Secure Flight beginning in November, 2004. The testing involved 15 million PNRs relating to flights flown domestically on every U.S. carrier in June, 2004. That test demonstrated that the system was effective in matching PNR data with data contained in terrorist watch lists and that the system can handle the expected load of more than 1.8 million passengers per day. The preliminary testing also enabled TSA to determine that it must obtain, at a minimum, an individual's full name and date of birth in order to perform an effective comparison of that individual against those individuals identified on the No-Fly and Selectee Lists. Testing showed that use of date of birth is helpful in distinguishing a passenger from an individual on a Federal watch list with the same or similar name and significantly reduced the number of false positive watch list matches.

In addition to the testing to determine TSA's ability to compare passenger information with data maintained by TSC, TSA is continuing with a separate set of testing involving commercial data. Our purpose is to test the Government's ability to verify the identities of passengers using commercial data and to improve the efficacy of watch list comparisons by making passenger information more complete and accurate using commercial data. In conducting commercial data testing, procedures have been put in place to ensure strict adherence by contractors and their personnel to privacy standards and data security protections. No decision has yet been made on whether commercial data will ultimately be used in Secure Flight. If TSA decides to use commercial data for Secure Flight, it will not do so until the agency publishes a new SORN and PIA announcing how commercial data will be used and how individuals' privacy will be

protected. TSA will not be using commercial data upon the initial rollout of Secure Flight.

Let me say a bit more about the importance TSA gives to incorporating privacy rights protections in the design of Secure Flight. The protection of privacy is an omnipresent concern as TSA tests, develops, and implements Secure Flight. We are resolute in our commitment to adhere to the letter and intent of the Privacy Act and applicable policies on privacy protection and are endeavoring to resolve all of the outstanding issues relating to privacy. Moreover, we have continuously consulted with various privacy advocates to seek best practices and share details about this important program, and we will continue to work with the DHS Privacy Officer on the privacy issues relating to Secure Flight.

As you are probably aware, recently, the Deputy Secretary requested the Department's Privacy Officer to assess the handling of PNR information and commercial data during the testing phase and to provide any recommendations about how to strengthen our focus on privacy protection as we continue testing and contemplate deployment of Secure Flight. The Deputy Secretary has made the same request of the Department's new Data Privacy and Integrity Advisory Committee. I met with this group in Boston last week to brief them and to solicit their counsel. Throughout our testing of commercial data, Government Accountability Office (GAO) and interested committees in Congress have been made fully aware of the details surrounding our goals and methodology in conducting this testing.

On June 22, 2005, TSA amended the scope of the SORN and PIA to clarify and describe with greater particularity the categories of records and categories of individuals covered by the Secure Flight Test Records system. The GAO also has conducted extensive assessments of Secure Flight, including recently our use of commercial data testing. TSA is cooperating fully to ensure that all privacy concerns are addressed in an appropriate manner.

TSA has employed data security controls, developed with the TSA Privacy Officer, to protect the data used for Secure Flight testing activities. The procedures and policies that are in place are intended to ensure that no unauthorized access to records occurs and that operational safeguards are firmly in place to prevent system abuses. Measures that are in place include the following:

- Access to private information is limited to only those TSA employees and contractors who have a "need to know" to perform their duties associated with Secure Flight operations;
- A real-time auditing function is part of this record system to track all who accesses information resident on electronic systems during testing, and all instances when records are transmitted between TSA and contractors are meticulously kept;
- Data is maintained at a secure facility, and the information is protected in accordance with rules and policies established by both TSA and DHS for

automated systems and for hard copy storage, including password protection and secure file cabinets;

- Each employee and contractor associated with the Secure Flight program has completed mandatory privacy training prior to beginning work on the program.

Many technical challenges remain as TSA continues its work on testing Secure Flight in preparation for implementation and deployment. To ensure that these hurdles are overcome, it is absolutely necessary that Congress fully support the request in the President's budget for FY06, which proposes that Secure Flight be funded at $81 million. I would emphasize that if the program is ultimately funded at levels comparable to the $66 million or $56 million in the bills that have been approved by the House and reported in the Senate that a delay in implementation will be unavoidable.

TSA recognizes the importance of having in place a redress system that is readily available to passengers. TSA has already developed and implemented a clearance protocol for persons who are flagged for additional screening due to the similarity of their names to those of individuals who are appropriately on the watch lists. A passenger may initiate the clearance protocol by submitting a completed Passenger Identity Verification Form to TSA headquarters. TSA reviews the submission and reaches a determination of whether these procedures may aid in expediting a passenger's check-in process for a boarding pass. It is important to emphasize, however, that this clearance process is distinct from the ongoing internal review process to ensure that persons do not remain on the watch lists if they are found not to pose a security threat. TSA's clearance process distinguishes passengers who are not a security concern from persons who are on the watch lists by placing their names and identifying information in a cleared portion of the lists. This information is transmitted to the airlines. Following TSA-required identity verification procedures, airline personnel can then quickly determine that these passengers are not the person of interest whose name is actually on the watch lists.

In conjunction with the Secure Flight program, TSA has charged a separate Office of Transportation Security Redress to further refine the redress process under the Secure Flight program. The redress process will be coordinated with other DHS redress processes as appropriate. Utilizing current fiscal year funding, resources have been committed to this Office to enable it to increase staffing and to move forward on this important work. TSA recognizes that additional work remains to ensure that there is a fair and accessible redress process for persons who are mistakenly correlated with persons on the watch lists, as well as for persons who do not in actuality pose a security threat but are included on a watch list.

In addition to the mandates of IRTPA, Section 522 of the Homeland Security Appropriations Act, 2005 (P.L. 108-334) requires TSA to satisfy and GAO to report that TSA has addressed ten areas of Congressional interest relating to the Secure Flight program. On March 28, 2005, GAO released a report concluding that while "TSA has not yet completed these efforts or fully addressed these areas, due largely to the current stage of the system's development", "TSA is making progress in addressing each of the

key areas." GAO also issued six recommendations to assist TSA in managing the risks associated with the implementation of the Secure Flight program:

1. Finalize the system requirements document and the concept of operations, and develop detailed test plans—establishing measures of performance to be tested—to help ensure that all Secure Flight system functionality is properly tested and evaluated. These system documents should address all system functionality and include system stress test requirements.

2. Develop a plan for establishing connectivity among the air carriers, CBP, and the TSA to help ensure the secure, effective, and timely transmission of data for use in Secure Flight operations.

3. Develop reliable life-cycle cost estimates and expenditure plans for Secure Flight—in accordance with guidance issued by the Office of Management and Budget—to provide program managers and oversight officials with information needed to make informed decisions regarding program development and resource allocations.

4. Develop results-oriented performance goals and measures to evaluate the effectiveness of Secure Flight in achieving intended results in an operational environment—as outlined in the Government Performance and Results Act—including measures to assess associated impacts on aviation security.

5. Prior to achieving initial operational capability, finalize policies and issue associated documentation specifying how the Secure Flight program will protect personal privacy, including addressing how the program will comply with the requirements of the Privacy Act of 1974 and related legislation.

6. Prior to achieving initial operational capability, finalize policies and procedures detailing the Secure Flight passenger redress process, including defining the appeal rights of passengers and their ability to access and correct personal data.

TSA has systematically proceeded within the framework outlined by GAO to address the ten areas of Congressional interest identified in P.L. 108-334. With regard to the fifth recommendation, TSA is absolutely committed to safeguarding personal privacy and to complying with the letter and intent of the Privacy Act of 1974. As I previously discussed, many safeguards are already in place, and as we learn more through our ongoing testing, we will devise and implement the appropriate measures and will be updating the associated documentation as illustrated by our actions last week in issuing a revised SORN and PIA.

CONCLUSION

The implementation of an improved program for pre-screening of passengers against watch lists, as identified by the 9/11 Commission and Congress, is a vitally important

mission and is a high priority for TSA and the Department. We appreciate the support that you have voiced for expeditious implementation of Secure Flight and your recognition of the program's great potential for further improving aviation security. We acknowledge the concerns over our progress in development of the program and other related issues and are heavily engaged in resolving issues of concern. We will continue to work with you and other interested Members and Committees in Congress on Secure Flight and will keep you apprised of important developments as they occur.

Mr. Chairman, Congresswoman Sanchez, and other Members of the Subcommittee, this concludes my prepared remarks. I would be pleased at this time to answer any questions.